

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application for:

J Eric Mowat

Application No.: 09/981,343

Filing Date: 10/15/2001

For: METHOD AND APPARATUS FOR
FORWARDING REQUESTS IN A
CACHE HIERARCHY BASED ON
USER-DEFINED FORWARDING
RULES

Examiner: Bilgrami, Asghar H

Group Art Unit: 2143

Confirmation no.: 5512

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

DECLARATION UNDER 37 C.F.R. §1.131

I, J Eric Mowat, hereby declare that:

1. I am the inventor of the above-captioned patent application ("the present application") and the subject matter which is described and claimed therein ("the present invention").
2. I was employed by Network Appliance, Inc. (now named NetApp, Inc.) at the time I invented the present invention.
3. NetApp, Inc. is the assignee of the present application and the present invention.
4. Prior to June 26, 2001, I conceived of the invention in this country, according to independent claims 1, 15, 26, 32, 34, 37, 49, and 58 of the present invention, as evidenced by Exhibit A. Exhibit A is dated prior to June 26, 2001.

5. The present invention was actually reduced to practice in this country prior to June 26, 2001, as evidenced by Exhibits A and B. Exhibit A, which is an administration guide for a product named "NetCache Appliance 5.0," shows that the present invention was implemented in the NetCache Appliance 5.0 product. Exhibit B provides a listing of release dates of various products released by NetApp, Inc. Herein, Exhibit B, in its unredacted form, indicates that the NetCache Appliance 5.0 product with the present invention included was operational and was released to end users prior to June 26, 2001, thus showing actual reduction to practice of the present invention prior to June 26, 2001.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the above-identified application or any patent issued thereon.

Respectfully submitted,

Date 1/28/09



J. Eric Mowat

EXHIBIT A

NetCache™ Appliance 5.0 Administration Guide

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support: <http://now.netapp.com>
Information email: info@netapp.com
Information Web: <http://www.netapp.com>

Part number 210-02587
October 2000

Table of Contents

| | | |
|------------------|---|------|
| | Preface | xvii |
| Chapter 1 | Routine Administration | 1 |
| | NetCache Appliance management utilities | 2 |
| | Using the NetCache Manager utility | 3 |
| | About the command-line interface | 5 |
| | Getting on-line information and help | 6 |
| | Changing the NetCache Appliance configuration | 8 |
| | Changing the NetCache Appliance host name | 9 |
| | Specifying NetCache port settings | 10 |
| | Halting, rebooting, and powering down the NetCache Appliance | 16 |
| | Backing up and restoring the NetCache Appliance configuration | 18 |
| | Configuring Autosupport | 25 |
| | Software licenses | 32 |
| Chapter 2 | Maintaining NetCache Administrative Security | 33 |
| | Managing NetCache Manager administrator accounts | 34 |
| | Managing access to the NetCache Appliance console | 37 |
| | Restricting administrative traffic to the NetCache Appliance | 38 |
| | Servicing non-HTTP traffic with tunneling | 42 |
| | Configuring the Allowed Tunnel Destination Ports option | 44 |
| Chapter 3 | Network Interface Configuration | 47 |
| | Section A: Managing network interfaces | 48 |
| | About network interfaces | 49 |
| | Network interface configuration | 50 |
| | Configuring a network interface | 55 |
| | Changing the state of an interface | 57 |

| | | |
|------------------|---|------------|
| | Section B: Managing virtual interfaces | 59 |
| | Understanding trunking. | 60 |
| | Virtual interfaces on a NetCache Appliance | 62 |
| | Creating a virtual interface | 65 |
| | Adding physical interfaces to a virtual interface | 68 |
| | Destroying a virtual interface. | 70 |
| | Section C: How NetCache interacts with a DHCP server | 71 |
| Chapter 4 | Routing on the NetCache Appliance | 73 |
| | Section A: About routing | 74 |
| | About routing on the NetCache Appliance. | 75 |
| | Configuring default and static routes. | 76 |
| | Configuring NetCache to work with a firewall. | 80 |
| | Section B: Binding types of traffic to specific interfaces | 81 |
| | Restricting client-to-NetCache traffic | 82 |
| | Balancing server-to-NetCache traffic. | 84 |
| | Section C: Configuring NetCache to use TCP large windows | 89 |
| Chapter 5 | NetCache Support for DNS. | 93 |
| | Section A: Basic DNS configuration on a NetCache Appliance | 94 |
| | Section B: Optional DNS configuration | 97 |
| | NetCache as a DNS proxy cache | 98 |
| | Handling domain names that are not fully qualified | 104 |
| | Handling DNS lookups for local servers | 108 |
| Chapter 6 | NetCache Support for FTP | 111 |
| | Overview of NetCache FTP support | 112 |
| | FTP object management | 113 |
| | Support for FTP connections | 115 |
| | Configuring FTP support | 117 |

| | | |
|----------------------|---|----------------|
| Chapter 7 | Using SNMP and the NetCache Appliance MIB | 121 |
| | About SNMP on the NetCache Appliance | 122 |
| | Configuring the SNMP agent. | 124 |
| | About the NetCache MIB. | 126 |
| Chapter 8 | Managing Disks | 131 |
| | Section A: RAID on the NetCache Appliance | 132 |
| | Understanding RAID | 133 |
| | Understanding disk addresses | 135 |
| | Understanding usable space on each disk | 137 |
| | Using fibre channel disks of various sizes | 138 |
| | Handling disk failure | 139 |
| | Section B: Disk Management on the NetCache Appliance | 142 |
| | Displaying the status and statistics of disks | 143 |
| | About adding and removing disks | 145 |
| | Adding disks to your system | 147 |
| | Removing disks from your system | 150 |
| | Replacing a failed disk on your system. | 152 |
| Chapter 9 | Managing Objects in the Cache | 155 |
| | Section A: How NetCache manages Web objects | 156 |
| | Specifying which Web objects are cached | 157 |
| | How long objects remain in the cache | 161 |
| | About the Force Refresh Rate option. | 166 |
| | Managing aborted requests | 168 |
| | Section B: How NetCache manages news objects | 169 |
| | Which news objects NetCache caches | 170 |
| | Specifying how often NetCache checks for new articles. | 171 |
| | Specifying how often NetCache checks for canceled articles | 174 |

Chapter 10

| | |
|---|-----|
| Request Resolution Hierarchies | 177 |
| Section A: Overview of request resolution hierarchies | 179 |
| About request resolution hierarchies | 180 |
| Examples: request distribution with and without a hierarchy | 185 |
| Request resolution when firewalls are deployed | 189 |
| What to read next | 190 |
| Section B: Single-member hierarchies | 191 |
| Understanding single-member hierarchies | 192 |
| Configuring a single-member hierarchy | 194 |
| Section C: Planning for hierarchies with multiple members | 201 |
| About planning for a multiple-member hierarchy | 202 |
| About identifying hierarchy members | 204 |
| About hierarchy request distribution methods | 210 |
| About hierarchy forwarding rules | 217 |
| Section D: Configuring hierarchies with multiple members | 224 |
| Step 1: Providing basic information about your NetCache Appliance | 226 |
| Step 2: Identifying members of your hierarchy | 228 |
| Step 3: Configuring hierarchy forwarding rules | 233 |
| Section E: Configuration scenarios | 239 |
| Scenario: hierarchy fully protected by a nontransparent firewall | 240 |
| Scenario: no intranet and a Web server outside the firewall | 243 |
| Scenario: company domain inside and outside the firewall | 247 |
| Scenario: requests distributed over multiple parents | 252 |
| Scenario: requests distributed over two firewalls | 258 |
| Scenario: hierarchy members handling specific types of requests | 261 |
| Scenario: hierarchy with a backup cluster | 267 |
| Section F: Controlling access by other proxy-cache servers | 271 |
| ICP ports and timeout period setup | 272 |
| ICP access controls | 273 |

| | |
|--|------|
| Limiting NetCache interfaces that accept ICP traffic | .276 |
| Section G: Troubleshooting the hierarchy configuration. | .278 |

Chapter 11

| | |
|--|------|
| Transparent Proxying. | .281 |
| Section A: About transparent proxying as a client access method. | .283 |
| Overview of transparent proxying | .284 |
| About using an L4 or L7 switch for transparent proxying | .288 |
| About using a router for transparent proxying | .290 |
| Requirements summary for deploying transparent proxying. | .298 |
| IP spoofing, IP forwarding, and URL forwarding | .300 |
| NetCache authentication for HTTP transparent proxying | .303 |
| About port settings for transparent proxying | .306 |
| Section B: Setting up transparent proxying—L4/L7 switch | .308 |
| Preparing for configuration | .309 |
| Configuring NetCache for transparency with an L4 or L7 switch | .311 |
| Testing transparency—DNS and an L4/L7 switch | .315 |
| Testing transparency—HTTP and FTP and an L4/L7 switch | .317 |
| Testing transparency—NNTP and an L4/L7 switch | .318 |
| Testing transparency—MMS and RTSP and an L4/L7 switch. | .321 |
| Troubleshooting transparency when using an L4 or L7 switch | .323 |
| Section C: Setting up transparent proxying—WCCP 2.0-based router. | .326 |
| Preparing for configuration | .327 |
| Configuring NetCache for transparent proxying with a WCCP router. | .329 |
| Testing transparency—DNS and a WCCP 2.0-based router | .334 |
| Testing transparency—FTP and HTTP and a WCCP 2.0-based router | .336 |
| Testing transparency—NNTP and a WCCP 2.0-based router | .340 |
| Testing transparency—MMS and RTSP and a WCCP 2.0-based router. | .344 |
| Troubleshooting transparency when using a WCCP 2.0-based router | .348 |
| Section D: Setting up transparent proxying—policy-based router | .354 |
| Preparing for configuration | .355 |

Preface

About this guide

This guide describes how to administer, manage, and optimize NetCache™ Appliances running NetCache 5.0 software. It provides information for the NetApp® C230, C630, C720, and C760 series NetCache Appliances.

For information about how to upgrade or service the system hardware, see the Field Service Guide for your NetCache Appliance model.

Audience

This guide is for system administrators who are familiar with computer networks, Web technology, and HTTP service. This guide assumes that customers planning to use the NetCache Appliance as a news cache have a basic understanding of NNTP and news service. This guide also assumes that customers planning to use the NetCache Appliance as a streaming media proxy have a basic understanding of RTSP, MMS, and streaming media service. This guide does not cover basic system administration topics such as IP addressing, routing, and network topology. It emphasizes the characteristics of the NetCache Appliance hardware and the NetCache software.

Command and keyboard conventions

You can enter NetCache Appliance commands on either the system console or from any client computer that can access the NetCache Appliance through Telnet.

When describing key combinations, this guide uses the hyphen (-) to separate individual keys. For example, “Ctrl-D” means pressing the “Control” and “D” keys simultaneously.

This guide uses the term “type” to mean pressing one or more keys on the keyboard. It uses the term “enter” to mean pressing one or more keys and then Enter. Also, this guide uses the term “Enter” to refer to the key that generates a carriage return, although the key is named “Return” on some keyboards.

This guide uses capitalization and some abbreviations to refer to the keys on the keyboard. (The keys on your keyboard might not be labeled exactly as they are in this guide.)

About this chapter

This chapter discusses the NetCache hierarchy feature, which enables you to set rules for how the NetCache Appliance you are configuring is to handle requests it cannot resolve. The hierarchy feature is flexible, enabling you to create simple to complex schemes.

Sections in this chapter

This chapter contains the following topics:

- ◆ Section A, “Overview of request resolution hierarchies,” on page 179
 - ❖ “About request resolution hierarchies” on page 180
 - ❖ “Examples: request distribution with and without a hierarchy” on page 185
 - ❖ “Request resolution when firewalls are deployed” on page 189
 - ❖ “What to read next” on page 190
- ◆ Section B, “Single-member hierarchies,” on page 191
 - ❖ “Understanding single-member hierarchies” on page 192
 - ❖ “Configuring a single-member hierarchy” on page 194
- ◆ Section C, “Planning for hierarchies with multiple members,” on page 201
 - ❖ “About identifying hierarchy members” on page 204
 - ❖ “About hierarchy request distribution methods” on page 210
 - ❖ “About hierarchy forwarding rules” on page 217
- ◆ Section D, “Configuring hierarchies with multiple members,” on page 224
 - ❖ “Step 1: Providing basic information about your NetCache Appliance” on page 226
 - ❖ “Step 2: Identifying members of your hierarchy” on page 228
 - ❖ “Step 3: Configuring hierarchy forwarding rules” on page 233
- ◆ Section E, “Configuration scenarios,” on page 239
 - ❖ “Scenario: hierarchy fully protected by a nontransparent firewall” on page 240
 - ❖ “Scenario: no intranet and a Web server outside the firewall” on page 243
 - ❖ “Scenario: company domain inside and outside the firewall” on page 247
 - ❖ “Scenario: requests distributed over multiple parents” on page 252
 - ❖ “Scenario: requests distributed over two firewalls” on page 258

- ❖ “Scenario: hierarchy members handling specific types of requests” on page 261
- ❖ “Scenario: hierarchy with a backup cluster” on page 267
- ◆ Section F, “Controlling access by other proxy-cache servers,” on page 271
 - ❖ “ICP ports and timeout period setup” on page 272
 - ❖ “ICP access controls” on page 273
 - ❖ “Limiting NetCache interfaces that accept ICP traffic” on page 276
- ◆ Section G, “Troubleshooting the hierarchy configuration,” on page 278

Section A: Overview of request resolution hierarchies

About this section

This section introduces you to the NetCache hierarchy feature. It defines a hierarchy and describes how you can use the hierarchy feature to customize handling of requests that your NetCache Appliance cannot resolve. It also contrasts request handling when a hierarchy is configured and when it is not. The information in this section is relevant for all administrators.

Topics in this section

This section contains the following topics:

- ◆ “About request resolution hierarchies” on page 180
- ◆ “Examples: request distribution with and without a hierarchy” on page 185
- ◆ “Request resolution when firewalls are deployed” on page 189
- ◆ “What to read next” on page 190

About request resolution hierarchies

Purpose of a request resolution hierarchy

The purpose of a request resolution hierarchy is to enable you to define what is to occur when the NetCache Appliance you are configuring cannot resolve a request—that is, what happens when a *cache miss* occurs.

The NetCache hierarchy feature imposes a logical structure on top of a physical network. This structure enables a NetCache Appliance to forward a request it cannot resolve to specific NetCache Appliances, third-party proxy-cache servers, and nontransparent firewalls for request resolution. Hierarchy configuration, therefore, affects traffic *outbound* from the NetCache Appliance on which you configure the hierarchy.

Note

When a transparent firewall exists, no explicit configuration is needed for requests to reach the Internet.

Why a cache miss occurs

A cache miss occurs in the following situations:

- ◆ A NetCache Appliance does not have the requested cacheable object in its cache.
- ◆ The requested object is noncacheable.
Refer to “Handling of noncacheable objects” on page 184 for details about the types of objects that are noncacheable.

Note

Streaming media data is always cacheable.

Behavior if no request resolution hierarchy is defined

If no request resolution hierarchy is configured on a specific NetCache Appliance, the appliance forwards the request over the default route.

Section A: Overview of request resolution hierarchies

Protocols and operating modes supported

The hierarchy feature supports the protocols and NetCache operating modes shown in the following table.

| NetCache Appliance operating mode | Hierarchy configuration issues |
|---|---|
| Web cache handling HTTP, FTP over HTTP, Gopher, and Tunnel (for example, HTTPS) | The protocols are fully supported. |
| Web cache handling FTP transparently | All hierarchy members handling transparent FTP must be NetCache Appliances. |
| Streaming media cache | Neighbors cannot be used. (A neighbor is a logical role that can be assigned to hierarchy members on a Web cache.) |
| Web accelerator | The hierarchy feature is not applicable. |
| News cache | <p>The hierarchy feature is not applicable.</p> <p>Note_____</p> <p>You can assign a parent-like relationship on the NNTP page by identifying the news server or another proxy-cache server from which the news cache is to obtain news.</p> _____ |

Rules-based hierarchy feature

The action that NetCache takes when the NetCache Appliance cannot resolve a request depends on the hierarchy forwarding rules that are configured on the NetCache Appliance. Hierarchy forwarding rules originate from the following sources:

- ◆ NetCache automatically turns on or off some rules based on how you configure specific options. Rule examples (in English) are as follows:
 - ❖ Send requests for local servers or the local domain directly to local servers.
 - ❖ Send requests for noncacheable objects directly to origin servers.

Section A: Overview of request resolution hierarchies

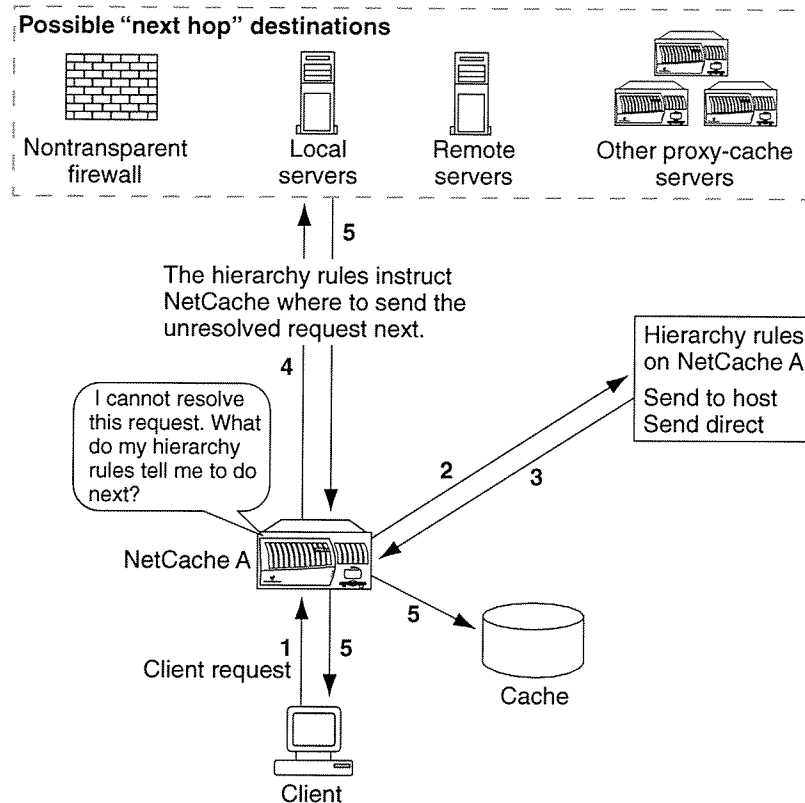
- ◆ NetCache turns on protocol-specific rules automatically based on the protocols supported by the hierarchy members you identify. Rule examples (in English) are as follows:
 - ❖ Load balance all unresolved RTSP requests over all hierarchy members that can handle RTSP.
 - ❖ Send an unresolved request to one or more nontransparent firewalls for delivery to the origin server on the Internet.
- ◆ NetCache uses custom rules that you create. You need to create custom rules only if your organization has specialized routing requirements. Rule examples (in English) are as follows:
 - ❖ Send unresolved requests from client IP address A to a specific member of the hierarchy you have configured.
 - ❖ Send unresolved requests to the backup host.

Hierarchy rules are discussed in detail in “About hierarchy forwarding rules” on page 217.

Illustrated overview of NetCache use of hierarchy forwarding rules

The following illustration shows the path of the request from the client to the NetCache Appliance, and from the appliance to its next-hop destination specified in a hierarchy rule. The next hop can be another proxy-cache server (NetCache or a third-party), a local or remote server, or a nontransparent firewall on the route to the Internet.

Section A: Overview of request resolution hierarchies



The numbers in the previous illustration show the sequence of events from the time the client makes the request to the time the client receives a response.

Note

For simplicity, the rules in the previous illustration are not shown as they would appear to NetCache.

Appliance-specific hierarchy configuration

You configure a hierarchy on an appliance-by-appliance basis. A particular NetCache Appliance hierarchy configuration can contain the host name of another proxy-cache server or a nontransparent firewall. However, the hierarchy configuration provides instructions *only* for the appliance on which the hierarchy is configured. No other NetCache Appliance, third-party proxy-cache server, origin server, or nontransparent firewall is aware of any hierarchy you configured on another NetCache Appliance.

Section A: Overview of request resolution hierarchies

Handling of noncacheable objects

The default NetCache behavior is to retrieve noncacheable objects directly from the origin server rather than sending the request through another proxy-cache server in the hierarchy. For this to occur, the connectivity of the NetCache Appliance must allow it to fetch noncacheable objects directly. If connectivity does not allow direct access to the origin server, the NetCache Appliance you are configuring must send the request to a hierarchy member that can reach the Internet.

The following objects are noncacheable:

- ◆ Objects with secure data
- ◆ Personal pages

Objects can be declared as noncacheable. For example:

- ◆ Administrators might designate their Web pages to be noncacheable to provide service that depends on maintaining state.
- ◆ As the NetCache administrator, you can specify for HTTP requests any URL substrings, MIME types, and object extensions that you do not want the NetCache Appliance to cache.

Note

Streaming media data is always cacheable.

Section A: Overview of request resolution hierarchies

Examples: request distribution with and without a hierarchy

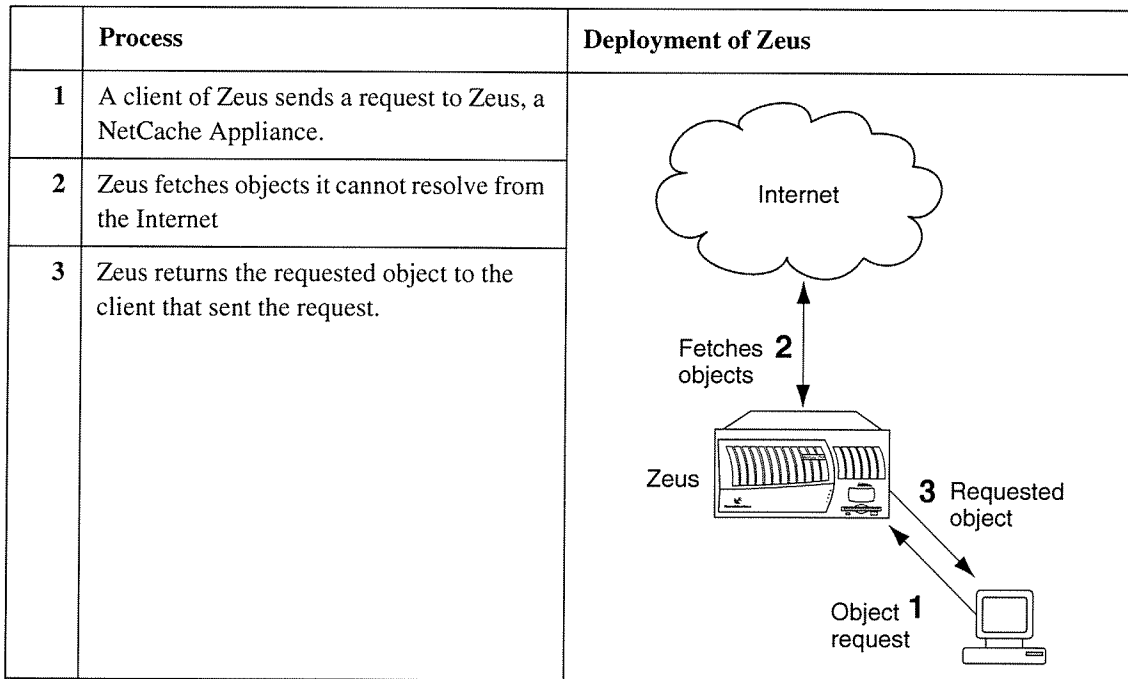
About this section

This section compares the request resolution capabilities of the same two NetCache Appliances with and without hierarchy configuration.

Example of request resolution when no hierarchy rules are configured

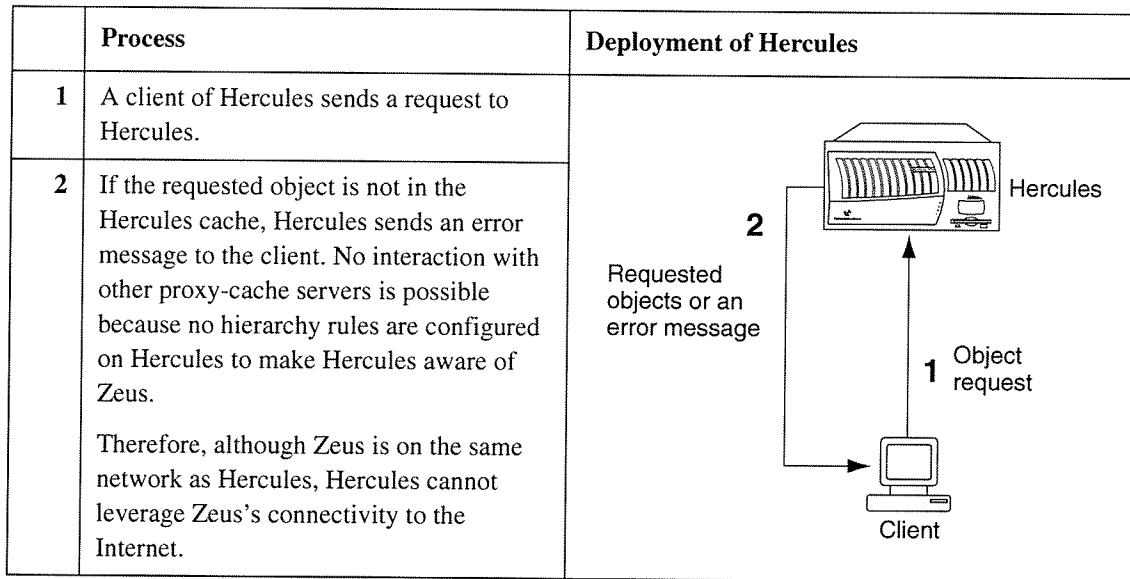
In the following example, two NetCache Appliances, Zeus and Hercules, reside on the same network. Zeus has direct connectivity to the network. Hercules, however, has no direct connectivity to the network. Because no hierarchy was configured on Hercules, the two appliances operate separately when trying to resolve requests.

The following illustration shows the request resolution flow for Zeus, which has direct access to the Internet.



Section A: Overview of request resolution hierarchies

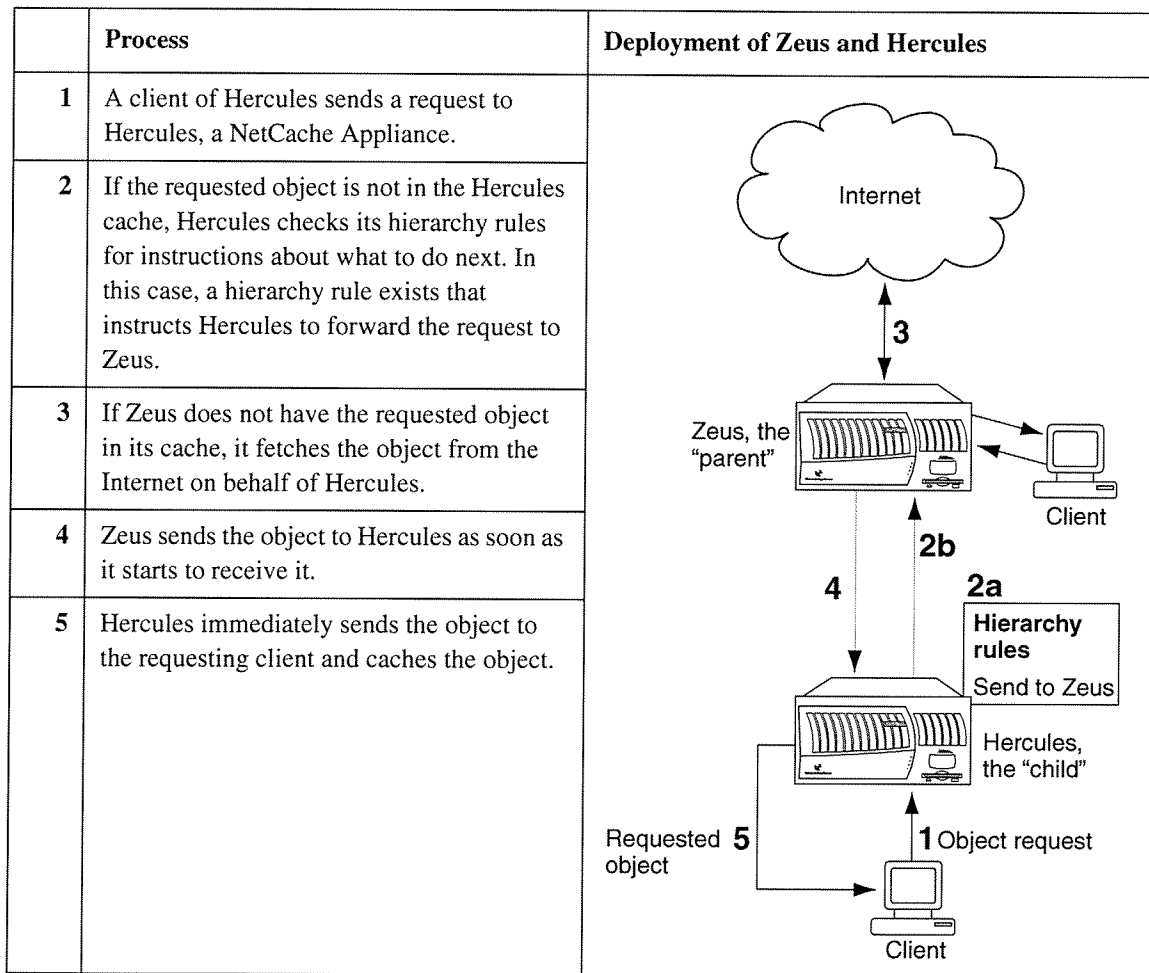
The following illustration shows the request resolution flow for Hercules, which does not have direct connectivity to the Internet.



Section A: Overview of request resolution hierarchies

Example of a request resolution when hierarchy rules are configured

The following illustration shows the same two NetCache Appliances as in the previous examples. In this case, however, hierarchy rules are configured on Hercules to leverage Zeus's ability to connect to the Internet.



Note—
For simplicity, the rule is not shown as it would actually appear to NetCache.

Section A: Overview of request resolution hierarchies

Notice that in the previous illustration, Zeus is labeled as the parent and Hercules is labeled as the child. When you configure a hierarchy on a NetCache Appliance, you identify the logical role that hierarchy members will play in the hierarchy. Specific characteristics for request resolution behavior are associated with each logical role in a hierarchy.

In this example, the hierarchy configured on Hercules identifies Zeus as a logical *parent* to Hercules. By identifying Zeus as a parent, Hercules can leverage Zeus's connectivity to the Internet because a parent can fetch objects on behalf of its logical *child*. The NetCache Appliance on which the hierarchy is configured, Hercules, in this case, is the child.

If you are configuring a single-member hierarchy, you do not need to know details about logical hierarchy roles. The procedures for a single-member hierarchy contain all the information you need to set up your hierarchy. If you are configuring a multiple-member hierarchy, you need to learn about hierarchy roles in "About identifying hierarchy members" on page 204.

Request resolution when firewalls are deployed

If your network includes a nontransparent firewall

Some requests must be sent to origin servers on the Internet to be resolved. Any nontransparent firewall running as a proxy must be explicitly identified as a member of the request resolution hierarchy. The reason is that a nontransparent firewall prevents a company's network devices from sending traffic directly to the Internet. The nontransparent firewall, therefore, becomes a hop on the way to the Internet origin servers. The firewall is responsible for connecting to the origin servers.

If your network includes a transparent firewall

You do not need to identify transparent firewalls in any NetCache Appliance hierarchy configuration. The reason is that NetCache automatically uses a NetCache Appliance default gateway to route requests to the Internet.

If your NetCache Appliance is outside your firewall

If you deploy a single NetCache Appliance outside your firewall, you do not need to configure a request resolution hierarchy. However, you might want to protect the NetCache Appliance from unauthorized access by other proxy-cache servers. Refer to Section F, "Controlling access by other proxy-cache servers," on page 271 for more information.

Section A: Overview of request resolution hierarchies

What to read next

Sections to read Depending on the type of hierarchy you are configuring, read the sections recommended in the following table.

| If you want the NetCache Appliance to... | You need to configure a... | Read... |
|--|----------------------------|--|
| Forward requests it cannot resolve to either one proxy-cache server or one nontransparent firewall | Single-member hierarchy | Section B, "Single-member hierarchies," on page 191 |
| Forward requests it cannot resolve to more than one proxy-cache server, more than one nontransparent firewall, or both | Multiple-member hierarchy | Section C, "Planning for hierarchies with multiple members," on page 201 Section D, "Configuring hierarchies with multiple members," on page 224 Section E, "Configuration scenarios," on page 239 |
| Interact with other proxy-cache servers over ICP | | Section F, "Controlling access by other proxy-cache servers," on page 271 |

Troubleshooting information is available in Section G, "Troubleshooting the hierarchy configuration," on page 278.

Section B: Single-member hierarchies

About this section

This section provides background information and procedures for configuring a hierarchy in which your NetCache Appliance forwards requests it cannot resolve to one proxy-cache server or one nontransparent firewall. Configuring a single-member hierarchy requires only a minimum amount of knowledge about how the hierarchy feature works. All information you need is included in this section.

Topics in this section

This section includes the following topics:

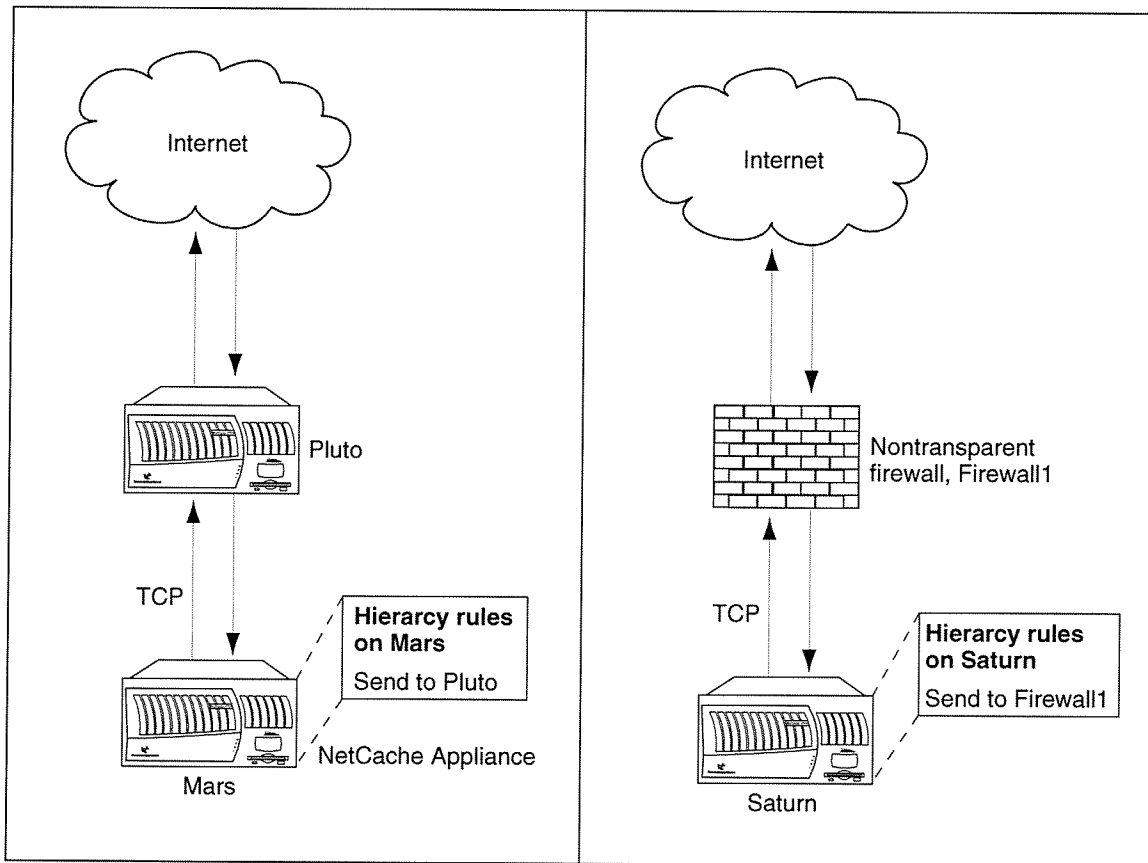
- ◆ “Understanding single-member hierarchies” on page 192
- ◆ “Configuring a single-member hierarchy” on page 194

Section B: Single-member hierarchies

Understanding single-member hierarchies

About single-member hierarchies

The simplest type of hierarchy is one that has only one hierarchy member, that is, only one proxy-cache server or only one nontransparent firewall. The following illustrations show the two types of single-member hierarchies. The illustration on the left shows the view of the hierarchy as it is configured on Mars, with only one member, the NetCache Appliance Pluto. The illustration on the right shows the view of the hierarchy as it is configured on Saturn, with a nontransparent firewall as the only member.



Section B: Single-member hierarchies

Configuring a hierarchy is advantageous in each deployment shown in the previous illustration because when the NetCache Appliance on which the hierarchy is configured cannot resolve a request, it forwards the request to its hierarchy member.

Note

You do not need to identify a transparent firewall as part of a hierarchy. NetCache automatically uses its default gateway to route requests to the Internet.

Mars is not identified as a member of the hierarchy configured on it. Likewise, Saturn is not identified as a member of the hierarchy configured on it. The reason is that a hierarchy configuration defines the action to be taken for requests *outbound* from the appliance on which the hierarchy is configured.

Why you might set up a single-member hierarchy with a proxy-cache server

You might set up a single-member hierarchy with another proxy-cache server for the following reasons:

- ◆ The NetCache Appliance you are configuring does not have direct connectivity to the Internet but another proxy-cache server does. (Refer to “Example of a request resolution when hierarchy rules are configured” on page 187.)
- ◆ You want another proxy-cache server to provide controls, such as content controls, for the NetCache Appliance you are configuring.

Connectivity requirements for noncacheable objects

By default, NetCache sends requests for noncacheable objects directly to origin servers. For this behavior to occur, the NetCache Appliance on which you are configuring the hierarchy must be able to reach the origin server directly. If it cannot, you must not select the check box in the “Bypass the Hierarchy for Noncacheable Objects” option on the Hierarchies - General page.

Configuring a single-member hierarchy

About this section

This section provides procedures for configuring a hierarchy with only one member—either a proxy-cache server (NetCache or third-party) or a nontransparent firewall. The following table shows the high-level tasks for configuring a single-member hierarchy.

| Order | High-level task | Read... |
|-------|--|--|
| 1 | Provide basic information about your hierarchy. | “Step 1: Configuring basic hierarchy settings” on page 195 |
| 2 | Identify and describe the member of your hierarchy, including any requirements for the NetCache Appliance you are configuring to authenticate to a hierarchy member. | “Step 2: Identifying the hierarchy member” on page 197 |

Note

You do not need to create hierarchy rules for a single-member hierarchy. The reason is that two options on the Hierarchy - General page control the rules for a single-member hierarchy. NetCache enables and disables the rules based on your selections on the General page.

For example, for a hierarchy with a nontransparent firewall, NetCache automatically provides a rule so that the NetCache Appliance on which the hierarchy is configured sends requests for local servers and the local domain directly to local servers.

Section B: Single-member hierarchies

Step 1: Configuring basic hierarchy settings

On the NetCache Appliance you are configuring, you must provide basic information about your hierarchy.

To configure basic hierarchy settings, complete the following steps.

| Step | Action |
|------|---|
| 1 | <p>In the NetCache Manage utility, select Setup tab > Hierarchies > General.</p> <p>Result: The Hierarchies - General page is displayed.</p> |
| 2 | <p>On the Hierarchies - General page, ensure that the Hierarchy Enable check box is selected.</p> <p>Note_____</p> <p>Disabling this control does not affect the configuration data entered for the hierarchy.</p> |
| 3 | <p>For the “Bypass Hierarchy for Noncacheable Objects” option</p> <ul style="list-style-type: none">◆ If your network includes a nontransparent firewall, ensure that this option <i>is not</i> selected.◆ If your network includes a transparent firewall, ensure that this option <i>is</i> selected. <p>Note_____</p> <p>For transparent firewalls, NetCache automatically uses its default gateway to route requests to the Internet.</p> <p>_____</p> <p>This option is directly linked with the NetCache default rule for handling noncacheable objects. If this option is selected, the noncacheable object rule is enabled and NetCache automatically sends requests for noncacheable objects directly to origin servers.</p> |

Section B: Single-member hierarchies

| Step | Action |
|------|--|
| 4 | <p>Select the Local Domain Enable check box and, if necessary, change the domain name in the “This Domain is Local to This NetCache Appliance” text box.</p> <p>You might, for example, want to enter a domain name that is less restrictive than the default domain name in the text box. For example, if the NetCache Appliance is in <i>lab.abc.com</i> but you want all of <i>abc.com</i> to be fetched directly, you would enter <i>.abc.com</i>.</p> <p>Note</p> <p>The domain name that is displayed in the domain name text box by default is the NetCache domain name that was entered during the setup program. Subsequent changes to the domain name on this page do not affect the DNS page. Similarly, changing the domain name on the DNS page does not affect this page.</p> |
| 5 | <p>Click Commit Changes at the bottom of the page.</p> <p>Result: You have finished configuring basic hierarchy settings. Next, identify your hierarchy member as described in “Step 2: Identifying the hierarchy member” on page 197.</p> |

Section B: Single-member hierarchies

Step 2: Identifying the hierarchy member

When you configure a hierarchy, you must identify and provide details about the nontransparent firewall or proxy-cache server that will be the hierarchy member.

To identify the member of your hierarchy, complete the following steps.

| Step | Action |
|------|---|
| 1 | <p>In the NetCache Manager utility, select Setup tab > Hierarchies.</p> <p>Result: The Hierarchies section of the Setup tab menu opens.</p> |
| 2 | <p>Select the link for the type of hierarchy member you are identifying, as follows:</p> <ul style="list-style-type: none">◆ If you are identifying a nontransparent firewall, select Hierarchies > Nontransparent Firewalls.◆ If you are identifying a proxy-cache server, select Hierarchies > Parents. <p>A parent is a logical role that enables the hierarchy member to fetch objects on behalf of the NetCache Appliance on which the hierarchy is configured. If the proxy-cache server that you identify as a parent is to fetch objects from the Internet, it must have the physical connectivity to access the Internet.</p> <p>Note _____ The NetCache Appliance that you are configuring is the logical child to the member you identify. However, you do not explicitly identify it as the child.</p> <p>Result: The Nontransparent Firewalls or the Parents page is displayed, with the Edit tab selected.</p> |
| 3 | <p>On the Nontransparent Firewalls page or the Parents page (as applicable), select the Add Firewall or Add Parent tab.</p> |
| 4 | <p>Enter in the Host Name text box the host name for the new hierarchy member.</p> |

Section B: Single-member hierarchies

| Step | Action |
|------|--|
| 5 | <p>In the “Ports Used to Contact This Host” option, change port numbers as appropriate.</p> <p>For MMS: If the host listens for MMS requests, the MMS port in this option must be 1755. If you want to be sure that the MMS port is not used, you can enter 0. No other port numbers are valid.</p> <p>For ICP: If you expect that this NetCache Appliance will use ICP to query to the proxy-cache server or nontransparent firewall you are identifying, ensure that the port number for ICP is correct for this host. For a nontransparent firewall, also ensure that</p> <ul style="list-style-type: none">◆ The echo port on the nontransparent firewall is turned on, if one exists.◆ The ICP port on the Firewalls page matches the port that the firewall is using to echo back UDP requests. <p>Status Monitor: Enter the number of the port on which the host is listening for health checks from this NetCache Appliance.</p> |
| 6 | <p>In the Host Supports option, select the check boxes for the protocols that this firewall or proxy-cache server can handle.</p> <p>NetCache uses HTTP to send nontransparent FTP, Gopher, and tunnel requests.</p> |
| 7 | <p>In the “Cache Objects from This Host” check box, select or clear the check box as desired.</p> <p>If this check box is not selected, the appliance you are configuring just proxies objects fetched by the proxy-cache server or nontransparent firewall. If you are concerned about disk space on your NetCache Appliance, you might not want to cache objects from some hosts, for example, objects from a local server.</p> |

Section B: Single-member hierarchies

| Step | Action |
|------|--|
| 8 | <p>In the “Monitor Status Through” option, select the protocol that you want NetCache to use to monitor the status of the host you are identifying.</p> <p>To determine whether to select TCP or HTTP, you need to know if the host has any restrictions that would affect the choice of the protocol that NetCache can use to check the host’s status. For example, a particular nontransparent firewall might allow only tunneling to it, not HTTP GET requests. In this case, you would need to select TCP.</p> |
| 9 | <p>In the Hierarchy Authentication option, identify the type of hierarchy authentication between this NetCache Appliance and the host, as follows:</p> <ul style="list-style-type: none">◆ None Select this option button if the host you are identifying does not require this NetCache Appliance, or clients connecting to this NetCache Appliance, to authenticate to it.◆ Pass Through the User Name and Password Supplied by the Client Select this option button if the host you are identifying requires an end user to provide a user name and password. <p>Note _____ This option is not applicable for transparent FTP.</p> <p>You must add the user name and password to the NetCache user database on this NetCache Appliance or to the LDAP, RADIUS, or NTLM server used by this appliance for authentication.</p> <ul style="list-style-type: none">◆ User Name and Password Required by this Host Select this option button if the host you are identifying requires this NetCache Appliance to supply a user name and password to connect to it. Obtain the user name and password from the administrator of the host you are identifying. <p>You must add the user name and password to the NetCache user database on this NetCache Appliance or to the LDAP, RADIUS, or NTLM server used by this appliance for authentication.</p> |

Section B: Single-member hierarchies

| Step | Action |
|------|---|
| 10 | Click Commit Changes at the bottom of the page. Result: Your hierarchy configuration is complete. |

Temporarily disabling a hierarchy

By unselecting the Hierarchy Enable option on the Hierarchies > General page, you can disable your hierarchy without clearing your configuration settings. You might, for example, want to disable the hierarchy when troubleshooting.

Section C: Planning for hierarchies with multiple members

About this section

This section contains information to help you plan how to configure a hierarchy that includes multiple members, that is, two or more proxy-cache servers or two or more nontransparent firewalls to which the NetCache Appliance you are configuring is to send requests that it cannot resolve.

Topics in this section

This section contains the following topics:

- ◆ “About planning for a multiple-member hierarchy” on page 202
- ◆ “About identifying hierarchy members” on page 204
- ◆ “About hierarchy request distribution methods” on page 210
- ◆ “About hierarchy forwarding rules” on page 217

Who should read this section

Read this section if you want to understand the capabilities of the NetCache hierarchy feature or if you know that you will set up a hierarchy with multiple members.

Section C: Planning for hierarchies with multiple members

About planning for a multiple-member hierarchy

What you need to plan

The following table summarizes planning activities for a multiple-member hierarchy.

| You need to... | Read... |
|---|--|
| Create an overall hierarchy plan and appliance-specific plans. | "Create both an overall plan and individual plans" on page 202 |
| Understand the modes and protocols that the hierarchy feature supports. | "Protocols and operating modes supported" on page 181 |
| Determine whether you need to identify each hierarchy member to NetCache as a logical parent, a logical neighbor, or a nontransparent firewall. | "About logical roles for hierarchy members" on page 204 |
| Determine whether you must create custom hierarchy rules or whether the NetCache-supplied hierarchy rules are sufficient for your organization. | "About hierarchy request distribution methods" on page 210 "About hierarchy forwarding rules" on page 217 |

Create both an overall plan and individual plans

Setting up a hierarchy with multiple members (proxy-cache servers or nontransparent firewalls) requires planning to ensure that you achieve the results that you intended. Plan your hierarchy scheme as follows:

- ◆ Create an overall request resolution plan for your organization.
Your overall plan needs to include information about how each NetCache Appliance in your organization is to interact with other proxy-cache servers and nontransparent firewalls to resolve requests.
- ◆ Implement your overall request resolution hierarchy plan by configuring each of your NetCache Appliances with its view of the hierarchy.

Section C: Planning for hierarchies with multiple members

Determining the number of members in a hierarchy

To determine the number of members in a hierarchy, consider the following factors:

- ◆ Your goals for request resolution
- ◆ How much traffic a particular proxy-cache server or nontransparent firewall can handle
- ◆ Physical location of devices that will be members of your hierarchy
- ◆ Protocols that a specific device can handle
- ◆ Whether you need load balancing
- ◆ Whether you have special requirements, for example, for specific members to handle specific protocol or request types

When determining the number of members in the hierarchy, do not count the NetCache Appliance you are configuring as a member of the hierarchy.

Are custom hierarchy forwarding rules needed?

You do not need to create hierarchy forwarding rules if no specific routing needs exist. For information about circumstances for which you must create custom hierarchy rules, refer to “What are hierarchy forwarding rules?” on page 217.

About identifying hierarchy members

About this section

When you configure a hierarchy, you must identify the members of the hierarchy. This section describes the logical roles that can be assigned to members of a hierarchy—a parent, a neighbor, or a nontransparent firewall—and the characteristics of each role. Characteristics associated with logical roles help you determine the appropriate role for a specific member. For example, a parent can fetch objects directly from the Internet, but a neighbor cannot.

Information you need to provide about a hierarchy member

When you identify and describe each member of the hierarchy, the information that you need to provide includes the following:

- ◆ Its logical role in the hierarchy—a parent, a neighbor, or a nontransparent firewall

Refer to “About logical roles for hierarchy members” on page 204.

- ◆ Protocols the hierarchy member supports
- ◆ Whether the host requires authentication

Refer to “About hierarchy authentication” on page 205.

Note

In previous releases of NetCache, whether the host was a member of a cluster was configured as part of the description of a particular cache host (hierarchy member). As of NetCache 5.0, the relationship between hierarchy members is defined as a part of setting up hierarchy rules.

About logical roles for hierarchy members

The following table shows the logical roles you can assign to members of a hierarchy and the main characteristics associated with each role. By matching your goals with the logical entity that can fulfill your goal, you can determine how to identify a particular host when you configure a hierarchy on your NetCache Appliance.

Section C: Planning for hierarchies with multiple members

| Logical characteristics of hierarchy members, by member type | Logical roles | | |
|--|---------------|----------|-------------------------|
| | Parent | Neighbor | Nontransparent firewall |
| Can accept a query for a requested object from the appliance you are configuring | Yes | Yes | No |
| Can fetch objects from the Internet on behalf of the appliance you are configuring | Yes | No | Yes |

Devices that can be a parent or a neighbor: The following types of network devices can be a parent or neighbor to the NetCache Appliance you are configuring:

- ◆ NetCache Appliances
- ◆ Third-party proxy-cache servers

You cannot specify neighbors for streaming media caches.

Note

Network Appliance does not recommend the use of neighbors. The reason is that the NetCache Appliance on which the hierarchy is configured always uses ICP to communicate with neighbors, which is not as efficient as using TCP for communication.

The child NetCache Appliance: When you identify a parent or nontransparent firewall as a member of the hierarchy, the appliance you are configuring is the logical *child* to that parent or nontransparent firewall. However, you do not include the host name of the child NetCache Appliance in the hierarchy configuration.

About hierarchy authentication

Authentication between proxy-cache servers works much the same as user authentication. If a specific hierarchy member requires a user name and password, the NetCache Appliance connecting to it must supply that user name and password. When you add a member in the hierarchy configuration, you must specify the type of hierarchy authentication required by the member or none if no hierarchy authentication is required. When you create your overall plan for the hierarchies to configure for your organization, you need to determine whether you want to require that lower level NetCache Appliances authenticate to other members of their hierarchy.

Section C: Planning for hierarchies with multiple members

Benefits of hierarchy authentication

Using hierarchy authentication can provide the following benefits:

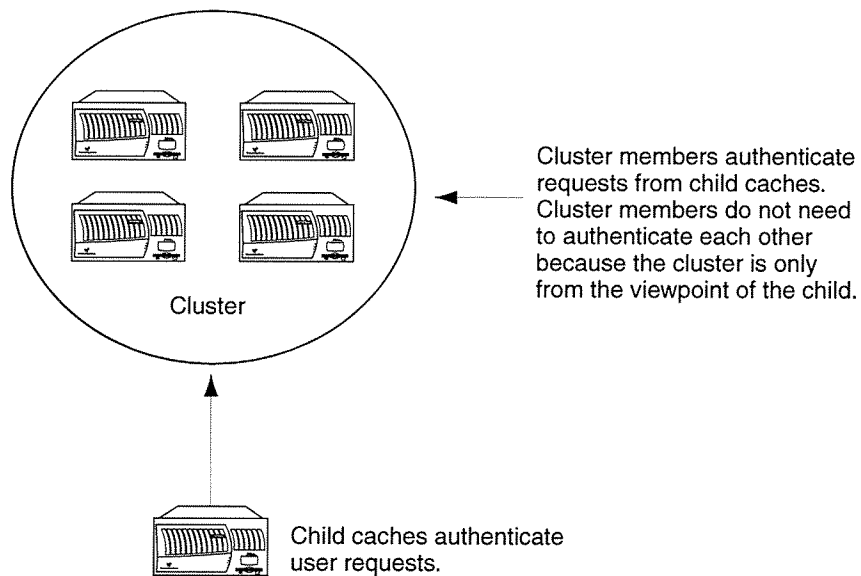
- ◆ Unauthorized proxy-cache servers cannot access a NetCache Appliance in the hierarchy.
- ◆ End users do not need to supply a user name and password for each proxy-cache server in the hierarchy that handles the user's request.
- ◆ Hierarchy members cannot bypass access controls.

Considerations for hierarchy authentication

If you decide to require hierarchy authentication, consider the following when planning your authentication scheme:

- ◆ How you want request records shown in log files
You must decide what kind of request records you want in the log files at each level in the hierarchy. Whether the log files on parents and cluster members show the child NetCache Appliance or the client depends on how you set up your hierarchy authentication scheme.
- ◆ The level at which to enable authentication and whether it should be user authentication or hierarchy authentication

The following illustration shows where authentication is needed in a typical hierarchy containing a cluster (group of proxy-cache servers over which requests are distributed).



Section C: Planning for hierarchies with multiple members

Use the following guidelines to help you decide where to enable the different types of authentication:

- ◆ Enable user authentication on the proxy-cache servers where user requests come in.
- ◆ Enable hierarchy authentication at higher levels in your hierarchy, where the requests that are being serviced are sent from proxy-cache servers lower in the hierarchy rather than from end users.

For example, you could require a child to authenticate to a parent cache. Similarly, you could require authentication between a child and cluster members.

It is generally not necessary to enable both user authentication and hierarchy authentication at every level in your hierarchy.

Section C: Planning for hierarchies with multiple members

Hierarchy authentication schemes

The following table shows the hierarchy authentication schemes and the effects of each scheme on the parent log files and the databases of the parent and child.

| Authentication scheme | Hierarchy authentication setting on the child | Parent log file information | Database requirements |
|--|--|--|--|
| The child must supply a user name and password required by the parent. | In the description of the parent, hierarchy authentication is set to "Use the User Name and Password Required by this Host." | All requests are sent from the child. | On the parent: The NetCache, LDAP, or RADIUS database must contain the user name and password that the child must use to authenticate to the parent. On the child: The NetCache, LDAP, or RADIUS database must contain the user name and password that the parent requires. |
| The child must pass through client user names and passwords to the parent. | In the description of the parent, hierarchy authentication is set to "Pass Through the User Name and Password Supplied by the Client." | Requests are sent from individual clients. | On the parent: Client user names and passwords must be in the database of each NetCache Appliance. |

Sharing user names and passwords

Multiple NetCache Appliances can use the same user name and password to log in to a parent that requires hierarchy authentication.

Section C: Planning for hierarchies with multiple members

Using hierarchy authentication and access controls together

You can use hierarchy authentication to allow or prevent access to another proxy-cache server in a hierarchy. In addition, you can use access controls on higher-level proxy-cache servers to more selectively allow or prevent access to particular content.

For example, an international ISP might want to prevent access to certain Web sites in the United States. To prevent their users from bypassing the NetCache Appliance, they set up a hierarchy authentication scheme. The configuration is as shown in the following table.

| NetCache Appliance A in country X (the child) | NetCache Appliance USA 1 (parent to A) |
|---|---|
| USA 1 is a parent. All requests for origin servers in the United States must be sent to USA 1. NetCache A must be set up to authenticate to USA 1. Access controls are set up to prevent access to the information on USA 1. | Requires A to authenticate to it. The database on USA 1 must contain the user name and password to be used by NetCache A. |

About hierarchy request distribution methods

About request distribution in a multiple-member hierarchy

For multiple-member hierarchies, NetCache provides several methods for controlling how and where requests are distributed among hierarchy members and origin servers. This flexibility enables you to optimize the routing of requests through a hierarchy.

Distribution methods are included in hierarchy rules

Each hierarchy forwarding rule must include information about how NetCache should distribute requests to which the rule applies. NetCache provides protocol-specific rules that include the most efficient distribution method. NetCache enables these rules by default, but disables them if you create custom protocol-specific custom rules. Most organizations can rely on default or predefined rules for their hierarchy distribution needs.

NetCache protocol-specific rules include distribution methods as follows:

- ◆ NetCache groups all parents you have identified into a parent cluster, by protocol.
- ◆ NetCache groups all firewalls you have identified into a firewall cluster, by protocol.
- ◆ For a mixture of types of hierarchy members (for example, parents and neighbors), NetCache declares the distribution method to be ICP. NetCache then communicates with those members through ICP.

Refer to “About hierarchy forwarding rules” on page 217 for more details about rules.

Hierarchy distribution methods

The following table shows the characteristics of each distribution method you can use to distribute the requests over a hierarchy. Details and illustrations of clusters and ICP communication follow the table.

Section C: Planning for hierarchies with multiple members

| Characteristics | Available distribution methods | | | |
|---|---------------------------------------|-------------------------------------|---|---|
| | Single host | Cluster (load balancing group) | ICP | Direct |
| Member roles | A parent or a nontransparent firewall | Parents or nontransparent firewalls | Multiple parents, a parent and a neighbor, or multiple nontransparent firewalls | Origin servers (local or on the Internet) |
| Load balancing over hierarchy members is allowed. | N/A | Yes | No | No |
| Communication protocol used. | TCP | TCP | ICP | TCP |
| Peer to peer failover is available. | No | Yes | No | No |
| A backup can be defined to provide failover. | Yes | Yes | Yes | N/A |

About clusters

A cluster is a group of proxy-cache servers or nontransparent firewalls over which the NetCache Appliance on which the hierarchy is configured distributes requests.

You can create a hierarchy rule to specify multiple proxy-cache servers or multiple nontransparent firewalls to be members of a logical *cluster*. The cluster acts as a parent to the NetCache Appliance you are configuring.

Benefits: The main benefits of using clusters are as follows:

- ◆ Load balancing

The NetCache Appliance on which you are configuring the hierarchy uses a proxy-selection algorithm to determine which hierarchy member in the cluster can best handle the request. The appliance sends the request only to that hierarchy member.

Section C: Planning for hierarchies with multiple members

You must have at least two cluster members handling the same protocol for load balancing to occur.

- ◆ **Failover**

If one member of a cluster goes down, the NetCache Appliance you are configuring sends the request to another cluster member.

- ◆ **Communication protocol**

Communication from the NetCache Appliance on which the hierarchy is configured to a cluster member is over TCP.

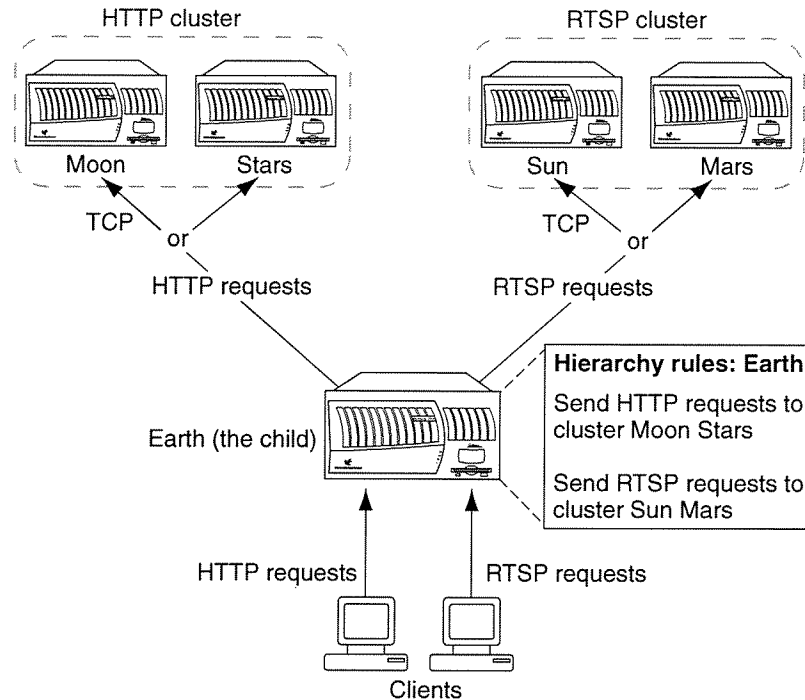
Belonging to multiple clusters: A proxy-cache server or nontransparent firewall can belong to more than one cluster if it handles multiple protocols. A single cluster cannot include both a nontransparent firewall and a proxy-cache server, however.

Examples of hierarchies with load balancing clusters

This section provides examples of hierarchies that include one or more clusters.

Clusters of proxy-cache servers: The following illustration shows a hierarchy configured on the child cache that includes two clusters.

Section C: Planning for hierarchies with multiple members

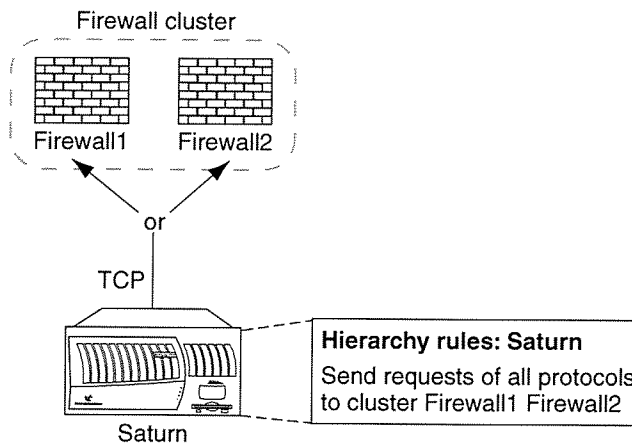


Details about the preceding illustration, which shows clusters as the distribution methods, are as follows:

- ◆ Number of parents
Earth, the child cache, has four parents: Moon, Stars, Sun, and Mars.
- ◆ HTTP cluster
Moon and Stars are in the HTTP cluster (because they handle only HTTP requests). Earth balances its unresolved HTTP requests over members of the HTTP cluster.
- ◆ RTSP cluster
Sun and Mars are in the RTSP cluster (because they handle only RTSP requests). Earth balances its unresolved RTSP requests over members of the RTSP cluster.
- ◆ Load balancing
For a given request, Earth determines which parent in the cluster can best handle the request.
- ◆ The communication protocol
Earth uses TCP to communicate with a cluster member.

Section C: Planning for hierarchies with multiple members

A firewall cluster: The following illustration shows a hierarchy that includes a cluster of two nontransparent firewalls. The hierarchy is configured on Saturn, which is the logical child in the hierarchy.



As in the previous illustration showing clusters of proxy-cache servers, Saturn balances the unresolved requests over the cluster members. Also, Saturn uses TCP to communicate with the firewall that will best handle the request.

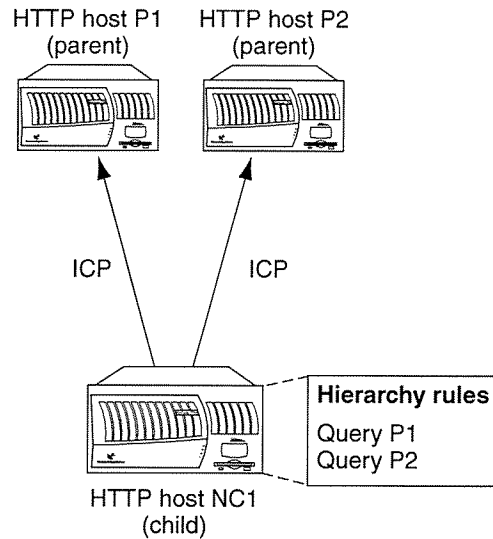
About using the ICP distribution method

ICP is best used for backward compatibility with Squid-based caches. Network Appliance recommends that, if you have multiple parents, you configure them to be part of a logical cluster rather than using ICP to communicate with parents individually. The reason is that ICP-based communication increases the amount of traffic without significantly increasing the hit rate. ICP is not an efficient scaling technique.

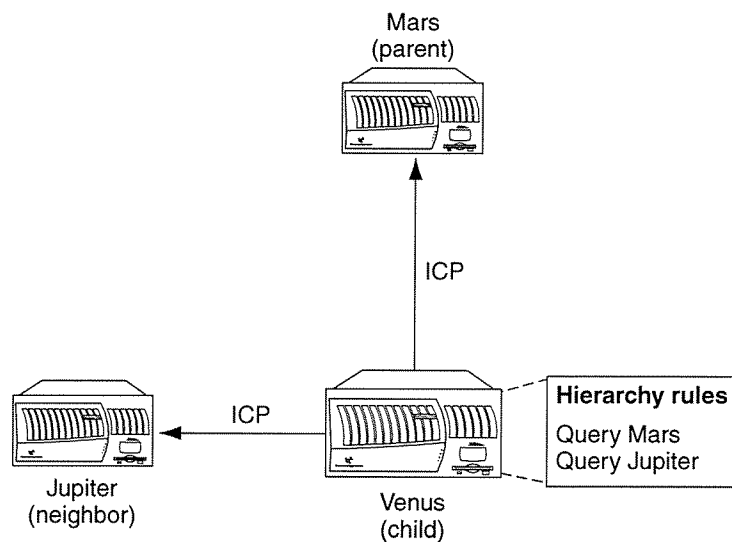
Examples of hierarchies using ICP

The following illustration shows a hierarchy in which the NetCache Appliance on which the hierarchy is configured (the child) queries each hierarchy member, through ICP, if the child cannot resolve a request.

Section C: Planning for hierarchies with multiple members



The following illustration shows a hierarchy in which the NetCache Appliance on which the hierarchy is configured (the child) queries each hierarchy member, through ICP, if the child cannot resolve a request. In this case, one of the hierarchy members is identified as a parent and the other is identified as a neighbor. If your hierarchy includes a neighbor, ICP is always used.



Section C: Planning for hierarchies with multiple members

Details about the ICP distribution method

When the distribution method is ICP, the following is true:

- ◆ Each hierarchy member is queried.
The child cache uses ICP to query each hierarchy member to determine if a member of the hierarchy has the requested object. Conversely, when two parents are part of a cluster, the child contacts only the proxy-cache server that can best handle the request.
- ◆ Load balancing is not supported.
If the hierarchy consists of multiple parents and the distribution method is ICP, the child cannot not balance over the two parent caches, unlike a cluster.
- ◆ Including neighbors is inefficient.
Network Appliance discourages the assignment of neighbors because the communication protocol used to contact neighbors is always ICP. Additionally, a neighbor, which is at the same level in the hierarchy as the child, cannot fetch objects from the Internet on behalf of the child cache. It is more efficient for a child to query a parent for an object because the parent can fetch objects on behalf of the child.

About hierarchy forwarding rules

About this section

This section describes hierarchy forwarding rules, which provide instructions to a NetCache Appliance about how to distribute requests that it cannot resolve. This section includes information about the following:

- ◆ NetCache-supplied hierarchy rules and the circumstances under which the NetCache supplied rules are enabled
- ◆ When you need to create custom rules

Refer to “Step 3: Configuring hierarchy forwarding rules” on page 233 for instructions about creating hierarchy rules.

Note

In previous releases of NetCache, hierarchy forwarding rules were hidden. Starting with NetCache 5.0, you can view all rules that NetCache provides and rules that you create. You might find viewing hierarchy rules to be helpful in testing your hierarchy configuration and troubleshooting.

Who should read this section

Read this section if you have special routing needs, which are described in “Only special routing needs require custom rules” on page 218, or if you want to understand rules that NetCache automatically provides for you.

What are hierarchy forwarding rules?

The NetCache hierarchy feature is rule-based. The NetCache Appliance on which the hierarchy is configured determines how to distribute requests it cannot resolve by checking the instructions in its hierarchy rules. Hierarchy rules can include protocols to which the rule applies, a condition under which a request is to be sent to a specified destination, and the hierarchy members to which the rule applies.

Hierarchy rules fall into the following main categories:

- ◆ Rules for sending unresolved requests to one or more hierarchy members
- ◆ Rules for sending unresolved requests directly to origin servers, which might be local to the NetCache Appliance or remote

A rule can apply to multiple hosts. You just include in the rule the host names for each host to which the rule applies.

Section C: Planning for hierarchies with multiple members

Note

If your “send direct” rule instructs your NetCache Appliance to send requests to the Internet, your appliance must have the physical connectivity to reach the Internet.

Only special routing needs require custom rules

Most organizations should be able to rely on the rules that NetCache supplies to handle their hierarchy request distribution needs. Typically, you do not need to create hierarchy rules unless you have specialized routing requirements, such as the following:

- ◆ You want a backup host or a backup cluster so that, if a primary host or cluster fails, NetCache sends the request to a backup host or cluster.
- ◆ You want NetCache to send requests of a particular protocol to a particular proxy-cache server, or you want NetCache to send (force) specific requests to a particular proxy-cache server if a particular condition exists.

Note

In releases prior to NetCache 5.0, the FORCE parameter in the Cache Host Domains option was used to send specific types of requests to specific hierarchy members. Starting with NetCache 5.0, creating a custom rule and ordering it so that it is executed before more general rules serves the same purpose.

If you create a custom rule that is specific to a protocol, the NetCache automatic rule for that protocol is automatically disabled. In addition to creating the specific rule, you must create a custom rule that provides instructions about to handle the requests of the same protocol that are not addressed by your specific rule. Refer to “Automatic rules that are provided” on page 220.

NetCache-supplied hierarchy rules

NetCache provides the following rules:

- ◆ Local domain
- ◆ Noncacheable
- ◆ Automatic protocol-specific rules
 - ❖ HTTP-to-all (includes HTTP, FTP, FTP over HTTP, Gopher, and Tunnel requests)
 - ❖ MMS-to-all
 - ❖ RTSP-to-all

Section C: Planning for hierarchies with multiple members

Whether NetCache activates any of these rules depends on information you provide when you configure the Hierarchy - General page and the protocols that you specify your hierarchy members to handle.

Local domain rule

Rule description: This rule delivers requests for the local domain to local servers.

How the rule is activated: This rule is enabled automatically if you select the Local Domain check box on the Hierarchy - General page for the “This Domain is Local to this NetCache Appliance” option. You do not need to add any elements to this rule.

Additional information: If your local domain is both inside and outside the nontransparent firewall, this rule does not affect requests for servers outside the firewall. You must create custom hierarchy rules to handle this situation. Refer to “Scenario: company domain inside and outside the firewall” on page 247 for an example of how to handle this situation.

Noncacheable rule

Rule description: This rule sends noncacheable objects directly to origin servers.

How the rule is activated: This rule is activated automatically if you select the “Bypass Hierarchy for Noncacheable Objects” check box on the Hierarchies - General page. You do not need to add any elements to this rule unless you have special routing requirements for noncacheable objects.

Additional information: If you want requests for a specific type of noncacheable object to be sent to a particular hierarchy member, you must create a custom rule. For example, you might want all tunnel requests sent to a specific host and requests for all other noncacheable objects sent directly to origin servers. In this case, you create your custom rule for sending tunnel requests to a specific host and move that rule before the general noncacheable rule in the hierarchy rule list. The reason is that you want the tunnel requests, which are noncacheable, to be invoked before the generic noncacheable rule.

Note

Streaming media data is always cacheable.

Section C: Planning for hierarchies with multiple members

Automatic rules that are provided

NetCache provides the following automatic rules:

- ◆ HTTP-to-all
- ◆ MMS-to-all
- ◆ RTSP-to-all

If you have no special routing requirements that require custom rules, you can rely on NetCache automatic, protocol-specific rules to distribute requests to origin servers. NetCache automatic rules are described in the next sections.

HTTP-to all automatic rule

Description: This rule sends all HTTP, FTP, FTP over HTTP, Gopher, and Tunnel requests to the origin server specified in the request.

Activation and deactivation: NetCache automatically includes all hierarchy members that you specified to handle HTTP if you do not create any other rules that apply to HTTP.

Distribution method: If multiple hierarchy members handle HTTP, NetCache specifies the distribution method as cluster unless one of those members is identified as a neighbor. If a neighbor exists, ICP is used to communicate to all the members that handle HTTP. Refer to “About logical roles for hierarchy members” on page 204 for information about the disadvantages of identifying hierarchy members as neighbors.

Additional information: If you want separate rules for any of the protocols that this rule represents, you must create a custom rule for the specific protocol. In addition to creating the specific rule, you must create a custom rule that provides instructions about how to handle HTTP requests that are not addressed by your specific rule. Refer to for information about the activation and deactivation of this rule.

MMS-to-all automatic rule

Description: This rule sends all MMS requests to the origin servers specified in the request.

Activation and deactivation: NetCache automatically includes all hierarchy members that you specified to handle MMS in this rule if you do not create any other rules that apply to the MMS protocol.

Distribution method: If multiple hierarchy members handle MMS, NetCache specifies the distribution method as cluster.

Section C: Planning for hierarchies with multiple members

Additional information: If you have special routing requirements for MMS requests, for example, to send MMS requests to a particular proxy-cache server if a specific condition exists, you must create two custom rules. One rule would be for the special condition and the other rule would be for the remainder of MMS requests.

RTSP-to-all automatic rule

Description: This rule sends all RTSP requests to the origin servers specified in the request.

Activation and deactivation: NetCache automatically includes all hierarchy members that you specified to handle RTSP in this rule if you do not create any other rules that apply to the RTSP protocol.

Distribution method: If multiple hierarchy members handle RTSP, NetCache specifies the distribution method as cluster.

Additional information: If you have special routing requirements for RTSP requests, for example, to send RTSP requests to a particular proxy-cache server if a specific condition exists, you must create two custom rules. One rule would be for the special condition and the other rule would be for the remainder of RTSP requests.

Elements in a hierarchy rule

A hierarchy rule can contain the following elements:

- ◆ Name
- ◆ On/off

You can turn off rules without losing the elements of the rule that you have configured.

- ◆ Protocols to which the rule applies

Identifying the protocols is necessary only if the rule does not apply to all protocols.

- ◆ Conditions under which the rule is to be executed

A rule can contain only one condition. If you need multiple conditions, you must create multiple rules.

Available condition elements are as follows:

- ❖ Noncacheable (objects)
- ❖ None (no conditions)
- ❖ Equals or does not equal: server IP address, server host name, server port, client IP address, client host name, URL, or beginning of URL.

Section C: Planning for hierarchies with multiple members

You can also specify your condition by using regular expressions.

- ◆ **Distribution method**

The distribution method specified in the rule determines how NetCache is to distribute requests over hierarchy members and origin servers. The distribution method can be any that is listed in the following table.

| Distribution method | Description |
|---|--|
| Direct | Send requests directly to the origin server. |
| Single host [select host] | Send requests of the specified type only to a specific proxy-cache server or nontransparent firewall. |
| Parent cluster or firewall cluster [select cluster members] | Load balance requests over multiple parents or multiple firewalls that handle the same protocol. |
| ICP [select hierarchy members] | Use ICP to communicate with hosts in the rule. If your hierarchy contains neighbors, ICP is always used to communicate with the neighbor. If a neighbor exists and NetCache is activating the automatic rule for HTTP, HTTP requests will be sent to all hosts after first querying using ICP. |

Execution order of rules

NetCache-provided hierarchy rules are automatically ordered for you. You can move rules up and down in the rules list, as necessary, so that the rules are executed in the proper order. The order of your hierarchy rules is important because NetCache executes the rules in the order in which they are listed, from the top to the bottom of the list. A general guideline is to list specific rules before general rules.

Example 1: Assume that you want all HTTPS requests to be tunneled to a specific host. You would create a custom rule for tunnel requests and list it before the more general noncacheable rule. The reason is that you want to be sure that the specific rule is executed before the general rule.

Example 2: Assume that you want to designate a backup host or a backup cluster. You move the rule for a backup host or a backup cluster lower in the rules list than the primary host rule or cluster rule. The reason is that you want the backup rule to be executed only if the primary rule fails.

Section C: Planning for hierarchies with multiple members

Examples of rules Refer to “Configuration scenarios” on page 239 for examples of how rules are configured for specific deployments.

Section D: Configuring hierarchies with multiple members

About this section

This section provides procedures for configuring a hierarchy with multiple members. The following table shows the high-level tasks for configuring a hierarchy, the relevant procedure in this section, and the information in the previous planning section that will help you to understand how to configure the procedure.

| Order | High-level task |
|-------|--|
| 1 | <p>Provide basic information about your hierarchy. All administrators configuring a hierarchy must provide this information.</p> <p>Procedure: “Step 1: Providing basic information about your NetCache Appliance” on page 226</p> |
| 2 | <p>Identify and describe members of your hierarchy, including any requirements for the NetCache Appliance you are configuring to authenticate to a hierarchy member. All administrators configuring a hierarchy must provide this information.</p> <p>Procedure: “Step 2: Identifying members of your hierarchy” on page 228</p> <p>Background information: “About identifying hierarchy members” on page 204 and “About hierarchy authentication” on page 205</p> |
| 3 | <p>Configure hierarchy forwarding rules, which determine where and under what circumstances a request is forwarded. Custom hierarchy rules are required only if you have special routing requirements.</p> <p>Procedure: “Step 3: Configuring hierarchy forwarding rules” on page 233</p> <p>Background information: “About hierarchy request distribution methods” on page 210 and “About hierarchy forwarding rules” on page 217</p> |

Section D: Configuring hierarchies with multiple members

Appliance-specific hierarchy configuration

You configure a hierarchy on an appliance-by-appliance basis. Use your overall plan for hierarchies at your organization to determine the specific configuration to provide for each NetCache Appliance on which you are configuring a hierarchy. The hierarchy configuration on a particular NetCache Appliance provides instructions *only* for the appliance you are configuring. No other NetCache Appliance, third-party proxy-cache server, or nontransparent firewall is aware of any hierarchy you configured on another NetCache Appliance.

Section D: Configuring hierarchies with multiple members

Step 1: Providing basic information about your NetCache Appliance

Configuring basic information about this NetCache Appliance

For all types of hierarchies, you must provide basic information on the Hierarchies - General page about how the NetCache Appliance you are configuring interacts with the network.

To provide basic information about this NetCache Appliance, complete the following steps.

| Step | Action |
|------|---|
| 1 | <p>In the NetCache Manager utility, select Setup tab > Hierarchies > General.</p> <p>Result: The Hierarchies - General page is displayed.</p> |
| 2 | <p>On the General page, ensure that the Hierarchy Enable check box is selected.</p> <p>Disabling this control does not affect the configuration data entered for this hierarchy. This option is enabled by default.</p> |
| 3 | <p>For the “Bypass Hierarchy for Noncacheable Objects” option</p> <ul style="list-style-type: none">◆ If you are identifying a nontransparent firewall, ensure that this option <i>is not</i> selected.◆ If your network includes a transparent firewall, ensure that this option <i>is</i> selected. <p>Note— For transparent firewalls, NetCache automatically uses its default gateway to route requests to the Internet.</p> <p>This option is directly linked with the NetCache default rule for handling noncacheable objects. If this option is selected, the noncacheable object rule is enabled and NetCache automatically sends noncacheable objects directly to origin servers. NetCache-supplied rules can be viewed on the Hierarchies > Forwarding Rules page. Section D, “Configuring hierarchies with multiple members,” on page 224 provides information about NetCache-supplied rules.</p> |

Section D: Configuring hierarchies with multiple members

| Step | Action |
|------|--|
| 4 | <p>Select the Local Domain Enable check box and, if necessary, change the domain name in the “This Domain Is Local to This NetCache Appliance” text box.</p> <p>You might, for example, want to enter a domain name that is less restrictive than the default domain name in the text box. For example, if the NetCache Appliance is in <i>lab.abc.com</i> but you want all of <i>abc.com</i> to be fetched directly, you would enter <i>.abc.com</i>.</p> <p>Note</p> <p>The domain name that is displayed in the domain name text box by default is the NetCache domain name that was entered during the setup program. Subsequent changes to the domain name on this page do not affect the DNS page. Similarly, changes to the domain name on the DNS page do not affect this page.</p> |
| 5 | Click Commit Changes at the bottom of the page. |
| 6 | Continue with your hierarchy configuration, following the procedure in “Step 2: Identifying members of your hierarchy” on page 228. |

Temporarily disabling a hierarchy

By unselecting the Hierarchy Enable option on the Hierarchies - General page, you can disable the hierarchy without clearing your configuration settings. You might want to disable the hierarchy when troubleshooting.

Step 2: Identifying members of your hierarchy

About identifying hierarchy members

You must identify all members of the hierarchy. You identify hierarchy members according to the logical role they are to play in the hierarchy—a parent, a neighbor, or a nontransparent firewall. You also provide information about that member, for example, protocols it handles, ports it is listening on, and any hierarchy authentication requirements. All administrators configuring a hierarchy must identify hierarchy members.

“About identifying hierarchy members” on page 204 provides information to help you understand the logical roles that you can assign hierarchy members. It also discusses hierarchy authentication, which you need to configure.

If you need to create hierarchy forwarding rules, you must identify hierarchy members before creating the rules. The reason is that you will select hosts to which the rule applies from the lists you use to create your rules. “About hierarchy forwarding rules” on page 217 provides information about when it is necessary to create hierarchy forwarding rules.

Identifying a hierarchy member

To identify and describe a member of the hierarchy, complete the following steps.

| Step | Action |
|------|---|
| 1 | In the NetCache Manager utility, select Setup tab > Hierarchies. Then select the Parents, Neighbors, or Firewalls link, depending on the logical role you plan to assign the hierarchy member you are identifying. Result: The Nontransparent Firewalls page, Parents page, or Neighbors page is displayed, with the Edit tab selected. |
| 2 | On the Nontransparent Firewalls, Parents, or Neighbors page (as applicable), select the Add tab. |
| 3 | In the Host Name text box, enter the host name for the new hierarchy member. |

Section D: Configuring hierarchies with multiple members

| Step | Action |
|------|--|
| 4 | <p>In the “Ports Used to Contact This Host” option, change port numbers as appropriate.</p> <p>For MMS: If the host listens for MMS requests, the MMS port in this option must be 1755. If you want to be sure that the MMS port is not used, you can enter 0. No other port numbers are valid.</p> <p>For ICP: If you expect that this NetCache Appliance will use ICP to query to the proxy-cache server or nontransparent firewall you are identifying, ensure that the correct port number for ICP is correct for this host. For a nontransparent firewall, also ensure that</p> <ul style="list-style-type: none">◆ The echo port on the nontransparent firewall is enabled, if one exists.◆ The ICP port on the Firewall page matches the port that the firewall is using to echo UDP requests. <p>Status Monitor: Enter the number of the port on which the host is listening for health checks from this NetCache Appliance.</p> |
| 5 | <p>In the Host Supports option, select the check boxes for the protocols that this firewall or proxy-cache server can handle.</p> <p>NetCache uses HTTP to send Gopher, tunnel, and nontransparent FTP requests.</p> |
| 6 | <p>In the “Cache Objects from This Host” option, select the check box as desired.</p> <p>If this check box is not selected, the appliance you are configuring just proxies objects fetched by the proxy-cache server or nontransparent firewall. If disk space is a concern for your NetCache Appliance, you might not want to cache objects from some hosts; for example, you might not want to cache objects from a local server.</p> |

Section D: Configuring hierarchies with multiple members

| Step | Action |
|------|---|
| 7 | <p>In the “Monitor Status through” option, select the protocol that you want NetCache to use to monitor the status of the host you are identifying.</p> <p>To determine whether to select TCP or HTTP, you need to know whether the host has any restrictions that would affect the choice of the protocol that NetCache can use to check the host’s status. For example, a particular nontransparent firewall might allow only tunneling to it, not HTTP GET requests. In this case, you would need to select TCP.</p> |
| 8 | <p>In the Hierarchy Authentication option, identify the type of hierarchy authentication that is required between this NetCache Appliance and the host (hierarchy member), as follows:</p> <ul style="list-style-type: none">◆ None Select this option button if the host you are identifying does not require this NetCache Appliance, or clients connecting to this NetCache Appliance, to authenticate to it.◆ Pass Through the User Name and Password Supplied by the Client Select this option button if the host you are identifying requires an end user to provide a user name and password. <p>Note _____ This option is not applicable for transparent FTP.</p> <ul style="list-style-type: none">◆ User Name and Password Required by This Host Select this option button and provide a user name and password if the host you are identifying requires this NetCache Appliance to supply a user name and password to connect to it. Obtain this user name and password from the administrator of the host you are identifying. <p>You must add this user name and password to the NetCache user database on this NetCache Appliance or to the LDAP, RADIUS, or NTLM database used by this appliance for authentication.</p> |
| 9 | Click Add. |

Section D: Configuring hierarchies with multiple members

| Step | Action |
|------|---|
| 10 | Continue to add hierarchy members as necessary, clicking Add after you enter data for each member. Your entries are only saved in memory until you commit your changes. |
| 11 | Click Commit Changes at the bottom of the page. |
| 12 | <p>If you have specialized request routing needs, for example, sending certain types of requests to a specific server, continue with “Step 3: Configuring hierarchy forwarding rules” on page 233.</p> <p>NetCache-supplied rules should be sufficient for many organizations. If you are not sure whether you need custom hierarchy forwarding rules, refer to “About hierarchy forwarding rules” on page 217.</p> |

Editing a hierarchy member's information

To edit the information about a particular host, complete the following steps.

| Step | Action |
|------|---|
| 1 | <p>From Setup tab > Hierarchies, select the link for the type of hierarchy member you are editing—Parents, Firewalls, or Neighbors.</p> <p>Result: The Nontransparent Firewalls page, Parents page, or Neighbors page is displayed, with the Edit tab selected.</p> |
| 2 | <p>Select the host from the list, then edit the host's information as necessary.</p> <p>Hierarchy members listed on the Edit tab page are members for which you have committed the configuration and members you have added during the current configuration session but have not yet committed.</p> <p>Refer to “Identifying a hierarchy member” on page 228 for details about fields on the host pages.</p> |
| 3 | Click Commit Changes at the bottom of the page. |

Section D: Configuring hierarchies with multiple members

Deleting a hierarchy member

The process of deleting a hierarchy member involves the following:

- ◆ If the host is included in a hierarchy rule, delete the host from the rule before deleting the host from a hierarchy member list. Refer to “About hierarchy forwarding rules” on page 217 and “Step 3: Configuring hierarchy forwarding rules” on page 233 for information about hierarchy rules and how to edit them.
- ◆ Delete the member from the Parents page, Neighbors page, or Nontransparent Firewalls page, as applicable.

To delete the information about a hierarchy member, complete the following steps.

| Step | Action |
|------|--|
| 1 | From Setup tab > Hierarchies, select the link for the type of hierarchy member you are deleting—Parents, Firewalls, or Neighbors. Result: The Nontransparent Firewalls page, Parents page, or Neighbors page is displayed, with the Edit tab selected. |
| 2 | Select the Delete tab. |
| 3 | Select the member from the list of members, then click Delete. |
| 4 | Continue to delete hierarchy members as necessary, clicking Delete after selecting each member. Your entries are only saved in memory until you commit your changes. |
| 5 | Click Commit Changes at the bottom of the page. |

Temporarily disabling a hierarchy

By unselecting the Hierarchy Enable option on the Hierarchies > General page, you can disable the hierarchy without clearing your configuration settings. You might want to disable the hierarchy when troubleshooting.

Section D: Configuring hierarchies with multiple members

Step 3: Configuring hierarchy forwarding rules

When you need to create custom rules

NetCache-supplied hierarchy rules should be sufficient for most organizations. However, custom hierarchy rules are necessary if you have special routing requirements. The main reasons for creating custom hierarchy rules are as follows:

- ◆ To send specific requests only to a specific hierarchy member

Note

In releases prior to NetCache 5.0, the FORCE parameter in the Cache Host Domains option was used to send specific types of requests to a specific hierarchy member. As of NetCache 5.0, creating a custom rule and ordering the rule so that it is executed before a more general rule serves the same purpose.

- ◆ If you have created a rule to send specific requests only to a specific hierarchy member
A NetCache protocol-specific automatic rule applies to all requests of the protocol. If you create a rule to send certain protocol-specific requests to a specific hierarchy member, you must also create a custom rule to handle the remainder of requests for that protocol.
- ◆ To group specific hierarchy members that handle a protocol into a smaller cluster rather than using the automatic rule to group all hosts that handle the same protocol into a cluster.
- ◆ To provide a backup host or backup cluster to be invoked only if the primary host or group rule fails
- ◆ If your company's domain exists both inside and outside your nontransparent firewall
Refer to "Scenario: no intranet and a Web server outside the firewall" on page 243 for details.

Prerequisites to configuring hierarchy rules

Identify the members of your hierarchy (parents, neighbors, and firewalls) and commit those configurations before creating custom hierarchy rules. The reason is that NetCache lists parents, neighbors, and firewalls in the host lists for creating rules.

Also, review the section "About hierarchy forwarding rules" on page 217 for details about NetCache-supplied hierarchy rules.

Section D: Configuring hierarchies with multiple members

Adding or editing custom hierarchy rules

To create or edit a custom rule, complete the following steps.

| Steps | Action |
|-------|--|
| 1 | <p>In the NetCache Manager utility Setup tab, select Hierarchies > Forwarding Rules.</p> <p>Result: The Hierarchy - Forwarding Rules page is displayed, with the Edit Rules tab selected.</p> |
| 2 | <p>If you are adding a rule, select the Add Rules tab.</p> <p>The fields for rule elements are the same on the Add Rules and Edit Rules tab pages. If you are editing a rule, change rule elements as necessary.</p> |
| 3 | <p>In the Rule Name text box, enter a name for your rule.</p> <p>No limit exists for the number of characters in a rule name. Rule names must be unique.</p> |
| 4 | <p>Select the Rule Enable check box to enable your rule.</p> |
| 5 | <p>In the Protocols option, select one or more protocols to which the rule is to apply or, if the rule applies to all protocols, do not select any protocols.</p> <p>If you do not select any protocols, the protocol is not a factor in determining whether your rule is invoked.</p> |
| 6 | <p>Select the option button for the condition under which the rule is to be executed, as follows:</p> <ul style="list-style-type: none">◆ None No conditions exist.◆ Noncacheable The rule applies to all noncacheable objects.◆ Phrase The rule applies to specific conditions, which you define in the next step. |

Section D: Configuring hierarchies with multiple members

| Steps | Action |
|-------|---|
| 7 | <p>If you selected the Phrase option button, do the following:</p> <ol style="list-style-type: none">From the first drop-down list, select Server IP address, Server host name, Server domain, Server port, Client IP address, URL, or Beginning of URL.From the second drop-down list, select either of the following: Select Equals if the rule is to be invoked if the value you supply in the text box matches exactly. Select Does not equal if the rule is to be invoked if the value you supply in the text box does not match exactly. Select Matches regular expression if the rule is to be invoked when the regular expression string that you enter in the text box matches the URL.In the text box, enter the value for the condition you specified. |
| 8 | <p>Select the distribution method and, as needed, hierarchy members to which the rule applies. The distribution method can be one of the following:</p> <p>Direct: If you want a rule for sending requests directly to a local server, local domain, or to origin server on the Internet (that is, you do not want to send requests to another proxy-cache server first), select Direct.</p> <p>Note _____ For this NetCache Appliance to be able to send cache misses to the Internet, this appliance must have direct connectivity to the Internet.</p> <hr/> <p>Single Host: If you want a rule that applies to only one host, select this distribution method, then select the applicable host from the drop down list.</p> |

Section D: Configuring hierarchies with multiple members

| Steps | Action |
|-------|--|
| | <p>Parent Cluster or Firewall Cluster: If you want load balancing over nontransparent firewalls or over proxy-cache servers that handle the same protocol, select Cluster as the distribution method. Then, from the drop-down list, select the hosts to which the rule applies.</p> <p>Load balancing can occur only if at least two hosts handling the same protocol are in the same cluster.</p> <p>ICP: If you want this NetCache Appliance to query parents, neighbors, or nontransparent firewalls individually through ICP, select ICP. Then, from the drop down list, select the hosts to which the rule applies.</p> <p>Communication with neighbors is always over ICP. If the hosts in your rule include a neighbor, you must select ICP as the distribution method for the rule.</p> <hr/> <p>Note Network Appliance does not recommend the use of ICP because ICP requires more overhead than TCP.</p> <hr/> |
| 9 | <p>If you are adding the rule, click Add.</p> <p>Continue to add rules as necessary, clicking Add after you enter data for each rule. Your entries are saved only in memory until you commit your changes.</p> |
| 10 | <p>Move your rule up or down in the rule list, as necessary.</p> <p>Rules are executed in order, from the top to the bottom of the list. Move specific rules before general rules in the list.</p> |
| 11 | <p>After you have finished adding or editing rules, click Commit Changes at the bottom of the page.</p> <p>Result: Your entries are saved to the NetCache configuration file.</p> |

Section D: Configuring hierarchies with multiple members

Reordering hierarchy rules

To reorder a hierarchy rule, complete the following steps.

| Step | Action |
|------|---|
| 1 | In the NetCache Manager Setup tab, select Hierarchies > Forwarding Rules. Result: The Hierarchies - Forwarding Rules page is displayed, with the Edit Rules tab selected. |
| 2 | In the Select a Rule list, select the rule whose order you want to change, then click Move Up or Move Down. You can look at the entire rule at once by clicking the View All Rules tab at the top of the page. You can move the rule only on the Edit Rules tab page, however. |
| 3 | Click Commit Changes at the bottom of the page. Result: Your changes are saved to the configuration file. |

Viewing hierarchy rules

To view hierarchy rules, complete the following steps.

| Step | Action |
|------|---|
| 1 | In the NetCache Manager Setup tab, select Hierarchies > Forwarding Rules. Result: The Hierarchies - Forwarding Rules page is displayed, with the Edit Rules tab selected. |
| 2 | You can view a rule in one of the following ways: <ul style="list-style-type: none">◆ On the Edit tab, select the name of the rule in the Current Rules list, then review the settings for the rule.◆ Click the View Rules tab. Rules are listed in the order they appear in the rules list. Automatic protocol-specific rules, which are last in the rules list, are separated out into a separate table under the Automatic Rules heading. Look for the On/Off setting to determine whether the rule is enabled. |

Section D: Configuring hierarchies with multiple members

Deleting hierarchy rules

You cannot delete NetCache-supplied rules. If you do not want a NetCache-supplied rule to be invoked, disable the rule. Refer to “Adding or editing custom hierarchy rules” on page 234.

To delete a rule, complete the following steps.

| Step | Action |
|------|---|
| 1 | In the NetCache Manager Setup tab, select Hierarchies > Forwarding Rules. Result: The Hierarchies - Forwarding Rules page is displayed, with the Edit tab selected. |
| 2 | Select the rule you want to delete from the Select a Rule list, then click Delete. |
| 3 | Click Commit Changes at the bottom of the page. |

EXHIBIT B



| | | | | |
|--|---------------------------------|-------------------------------|------------------------------|-----------------------|
| My NOW | Service and Support | Education and Consulting | Reseller and Partner | Communities |
| Technical Assistance and Documentation | Software Download | My NetApp Products | Product and Support Programs | Audit Management Tool |
| Download Software ToolChest | System Firmware Release Advisor | Backup Certification Matrices | | |
| Disk Drive Firmware | Release Comparison | Disk Shelf Firmware | | |

[Home](#) | [Feedback](#) | [Alerts](#) | [My Profile](#) | [Logout](#)

Software Change Log - 2006 and before

► [Go to Download Software](#)

► [Go to Current Software Change Log](#)

| Software | Date | Reason for Change |
|------------------------------------|------------|--|
| SnapManager for Oracle | [Redacted] | Publish SnapManager 2.0 for Oracle as First Customer Shipment release |
| VFM | [Redacted] | Publish VFM 5.8.1 as First Customer Shipment release |
| NetCache Appliance | [Redacted] | Publish NetCache 6.1.1RC1 as a Release Candidate |
| NearStore VTL | [Redacted] | Publish NearStore VTL 5.1 as a General Availability release |
| SnapDrive for Windows | [Redacted] | Publish SnapDrive 4.2.1 for Windows as First Customer Shipment release |
| SnapManager for Exchange | [Redacted] | Publish SnapManager 4.0 for Exchange as First Customer Shipment release |
| Data ONTAP | [Redacted] | Publish Data ONTAP 7.2.1 as General Availability release |
| TDPS | [Redacted] | Publish TDPS as General Availability release |
| SnapDrive for UNIX | [Redacted] | Publish SnapDrive 2.2 for UNIX as First Customer Shipment release |
| Data ONTAP GX | [Redacted] | Publish Data ONTAP GX 10.0.1 as General Availability release |
| DataFabric Manager | [Redacted] | Publish DataFabric Manager 3.4.1 as First Customer Shipment release |
| NetCache | [Redacted] | NetCache 6.0.4 moves to General Deployment release |
| Data ONTAP GX | [Redacted] | Publish Data ONTAP GX 10.0 as General Availability release |
| FCP Host Utilities (Attach Kits) | [Redacted] | Publish FCP Solaris Host Utilities 4.0 as First Customer Shipment release |
| FC and iSCSI Multipath I/O | [Redacted] | Publish Data ONTAP DSM 3.0 for Windows MPIO as First Customer Shipment release |
| Data ONTAP GX | [Redacted] | Publish Data ONTAP GX 10.0RC5 as Release Candidate |
| iSCSI Host Utilities (Attach Kits) | [Redacted] | Publish iSCSI QLogic 1.5 Host Utilities as General Availability release |
| SnapDrive for Windows | [Redacted] | Publish SnapDrive 4.2 for Windows as First Customer Shipment release |
| NetApp Host Agent | [Redacted] | Publish NetApp Host Agent 2.3.2 as General Availability release |

| | | |
|-----------------------------|------------|--|
| DataFabric Manager | [Redacted] | Publish DataFabric Manager 1.0 for Windows as General Availability release |
| Data ONTAP | [Redacted] | Publish Data ONTAP 6.1R1 as First Customer Shipment Release for the F630, F700 series, F800 series, and F85 |
| Data ONTAP | [Redacted] | Publish Data ONTAP 6.0.2R1 as First Customer Shipment Release for the F630, F700 series, F800 series, and F85 |
| NetCache Appliance | [Redacted] | Publish NetCache Appliance 5.1 as First Customer Shipment Release for the C700 series, C1100, C1105, C3100 and C6100 |
| Data ONTAP | [Redacted] | Publish Data ONTAP 6.1 as First Customer Shipment Release for F630, F700 series, F800 series, and F85 |
| Data ONTAP | [Redacted] | Publish Data ONTAP 6.0.2 as First Customer Shipment Release for F630, F700 series, F800 series, and F85 |
| Data ONTAP | [Redacted] | Data ONTAP 6.0.1R3 moves to General Availability Release for F630, F700 series, F800 series, and F85 |
| Data ONTAP | [Redacted] | Data ONTAP 5.3.7R3 moves to General Availability Release for F200, F300, F500 series |
| NetCache Appliance | [Redacted] | Publish NetCache Appliance 5.0.1R2 as Recommended Release for C600 series, C700 series, C1100, C1105, C3100, and C6100 |
| Data ONTAP | [Redacted] | Publish Data ONTAP 6.0.1R3 as Early Access F600 and F700 series, and as Recommended Release for F800 series and F85 |
| Data ONTAP | [Redacted] | Publish Data ONTAP 5.3.7R3 as Early Access F200, F300, F500 series |
| Data ONTAP | [Redacted] | Publish Data ONTAP 6.0.1R2 as Early Access F600 and F700 series, and as Recommended Release for F800 series and F85 |
| NetCache Appliance | [Redacted] | Publish NetCache Appliance 5.0.1R1 as Early Access for C600 series, C700 series, C1100, C1105, and C6100 |
| Data ONTAP | [Redacted] | Publish Data ONTAP 6.0.1R1 as Early Access for F630, F700 series, F840 |
| Data ONTAP | [Redacted] | Publish Data ONTAP 5.3.7R2 as Early Access |
| Data ONTAP | [Redacted] | Publish Data ONTAP 6.0R2 as Early Access for F760 |
| Data ONTAP | [Redacted] | Publish Data ONTAP 5.3.7R1 as Early Access |
| SnapManager | [Redacted] | Publish SnapManager 1.0.1 as Early Access |
| SecureAdmin for NetCache | [Redacted] | Publish SecureAdmin 2.1.1 for NetCache Appliance 5.0.x as Recommended release |
| ApplianceWatch for Tivoli | [Redacted] | Publish ApplianceWatch 1.0 for Tivoli Enterprise as Recommended release |
| Data ONTAP | [Redacted] | Publish Data ONTAP 5.3.7 as Early Access for F200 series, F300 series, F500 series, F630, F700 series, F840, and F840c |
| SecureAdmin for Data ONTAP | [Redacted] | Publish SecureAdmin 2.1.1 for Data ONTAP 6.0.x as Recommended Release for C1100 |
| NetCache Appliance | [Redacted] | Publish NetCache Appliance 4.1.2 as Recommended Release for C1100 |
| X <u>NetCache Appliance</u> | [Redacted] | Publish <u>NetCache Appliance 5.0 as Early Access for C600/C700/C1100/C6100 series</u> |